Checklist
For the Assessment of Safety Analysis and Design Software and Firmware
at Defense Nuclear Facilities

Page: 1 of 1

Deleted: 16

Inserted: 16

Deleted: 16

1. **Prepared by:**	2. **Date Prepared:**	3. **Type of Checklist:** Software, DNFSB □ External □ Internal
4. **Organization Evaluated:** **System Evaluated:**	5. **Evaluation Dates:**	6. **Source/Requirements Document:** DNFSB Recommendation 2002-1 Implementation Plan CRAD - 4.2.4.1, Rev 3, *RLB additions*

7. **Checklist Completed by:**

Assessor: ______________________ ______________________ ______________________

Print/Type Name Signature Date

8. **Personnel Contacted:**

Topical Area:	**Objective:**
4.1 Software Requirement Description	Analysis and design software functions, requirements, and their bases are defined, documented *and controlled*.

Criteria	**Comments/Notes/ Results**
1. The functional and performance requirements for the analysis and design software are complete and detailed to perform software design. **2.** The *Software Requirement Description* (SRD) is reviewed, controlled, and maintained.	
3. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.	

Software Requirement Description

Deleted: 16

Inserted: 16

Deleted: 16

Approach:

Determine the existence of SRD documentation, either as a standalone document or embedded in another document, and ensure that it specifies, as applicable, the following:

- Functionality - the functions the software is to perform,
- Performance - the time-related issues of software operation such as speed, recovery time, and response time,
- Design constraints imposed on implementation-phase activities - any elements that will restrict design options,
- Attributes - non-time-related issues of software operation such as portability, acceptance criteria, access control, and maintainability, and
- External interfaces - interactions with people, hardware, and other software.

Determine whether the documents containing the SRD are controlled under configuration change control and document control processes. Verify that the SRD is reviewed and updated as necessary for completeness, consistency, and feasibility for developing a usable code.

Identify the standards and guidelines from applicable site/facility procedures, Federal, or industry standards that are applied to the development of the software. Determine their appropriateness and adequacy for the specific analysis and design software under assessment.

If the above requirements are not available, the perceived software requirements may be identified through available documentation and discussions with the program developer, users, and sponsor. These perceived requirements would then be used as the basis for other topical area assessment activities.

Checklist
For the Assessment of Safety Analysis and Design Software and Firmware
at Defense Nuclear Facilities

Topical Area:	**Objective:**
4.2 Software Design Description	The *Software Design Description* (SDD) depicting the major components of the software design is defined, documented *and controlled*.
Criteria	**Comments/Notes/ Results**
1. All software-related requirements are implemented in the design.	
2. All design elements are traceable to the requirements.	
3. The SDD is reviewed, controlled, and maintained.	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software Design Description

Approach:

Review the appropriate documents, such as vendor specifications for analyzing and designing software, a description of the components and subcomponents of the software design, including databases and internal interfaces, etc. The design may be documented in a standalone document such as an SDD or embedded in other documents. The SDD should contain the information listed below:

- A description of the major safety components of the software design as they relate to the software requirements
- A technical description of the software with respect to control flow, control logic, mathematical model, and data structure and integrity
- A description of the allowable or prescribed ranges for inputs and outputs
- A description of error handling strategy and use of interrupt protocols
- The design should be described in a manner suitable for translating into computer codes

Determine whether the documents containing the software requirement description are controlled under configuration change control and document control processes. Verify that these documents are reviewed and updated as necessary for completeness, consistency, technical adequacy, and correctness.

In instances where the software the design is not available, the contractor may be able to construct a design summary on the basis of available program documentation, review of the source code (if applicable), and information from the facility staff. Care should be taken to ensure that such a design summary is consistent with the complexity and importance of the software to the safety functions.

Checklist
For the Assessment of Safety Analysis and Design Software and Firmware
at Defense Nuclear Facilities

Topical Area:	Objective:
4.3 Software User Documentation	Software documentation is available *and controlled* to guide the user in installing, operating, managing, and maintaining the software.

	Criteria	Comments/Notes/ Results
1.	The system requirements and constraints, installation procedures, and maintenance procedures such as database fine-tuning are clearly and accurately documented.	
2.	Any operational data system requirements and limitations are clearly and accurately documented.	
3.	Documentation exists to aid the users in the correct operation of the software and to provide assistance for error conditions.	
4.	Appropriate software design and coding documentation to assist in any future software modifications is defined and documented.	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software User Documentation

Approach:

The team will review the user's manual and related documents. These documents may exist either as a standalone document or embedded in other documents. The user documentation should contain:

- User instructions that contain an introduction, a description of the user's interaction with the software, and a description of any required training necessary to use the software
- Input and output specifications appropriate for the function being performed
- A description of error messages or other indications as a result of improper input or system problems and user response
- Information for obtaining user and maintenance support
- A description of system requirements and limitations such as operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software
- A description of any system requirements or limitations for operational data, such as file sizes
- Recommendations for routine database maintenance and instructions for performing this maintenance
- Design diagrams, structure or flow charts, pseudo code, and source code listings necessary for performing future modifications of custom software

Topical Area:	Objective:
4.4 Software Verification and Validation	The software V&V process is defined and performed, and related documentation is maintained to ensure that: (a) the software adequately and correctly performs all intended functions; (b) V & V is performed by persons not directly involved in generating the software code (c) the software does not perform any unintended function.
Criteria	**Comments/Notes/ Results**
1. All analysis and design software requirements and design have been verified and validated for correct operation using testing, observation, or inspection techniques.	
2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation, or inspection techniques.	

Deleted: 16

Inserted: 16

Deleted: 16

Formatted: Bulletsand Numbering

Deleted: 16

Inserted: 16

Deleted: 16

Software Verification and Validation

Approach:

Review the software V&V documentation, either as a standalone document or embedded in another document, to determine if:

- The tasks and criteria are documented for verifying the software in each development phase and validating it at completion,
- The hardware and software configurations pertaining to the software V&V are specified,
- Traceability to both software requirements and design exists,
- Results of the V&V activities, including test plans, test results, and reviews are documented,
- A summary of the status of the software's completeness is documented,
- Changes to software are subjected to appropriate V&V,
- V&V is complete, and all unintended conditions are dispositioned before software is approved for use and,
- V&V is performed by individuals or organizations that are sufficiently independent.

Checklist
For the Assessment of Safety Analysis and Design Software and Firmware
at Defense Nuclear Facilities

Topical Area:	Objective:
4.5 Software Configuration Management	The Software Configuration Management (SCM) process and related documentation for safety analysis and design software, including calculational software, are defined, maintained, and controlled.
Criteria	**Comments/Notes/ Results**
1. All software components and products to be managed are identified *and controled.*	
2. For those components and products, procedures exist to manage the modification and installation of new versions.	
3. Procedures for modifications to those components and products are followed *and controled.* .	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software Configuration Management

Approach:

Review appropriate documents, such as applicable procedures related to software change control, to determine if a SCM process exists and is effective. This determination is made based on the following actions.

- Verify the existence of an SCM plan, either in standalone form or embedded in another document
- Verify that a configuration baseline is defined and that it is being adequately controlled
- Verify that configuration items such as operating systems, source code components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, documents containing software requirements, software design, software V&V procedures, test plans, and procedures have been identified and placed under configuration control
- Review procedures governing change management, including installation of new versions of the software components and new releases of acquired software
- Review software change packages and work packages to ensure that:
  (1) possible impacts of software modifications are evaluated before changes are made,
  (2) various software system products are examined for consistency after changes are made,
  (3) software is tested according to established standards after changes have been made
- Verify by sampling that documentation affected by software changes accurately reflects all safety-related changes that have been made to the software
- Interview a sample of cognizant line, engineering, and QA managers and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design, safety basis, and software changes in a formal, disciplined, and auditable manner.

Checklist
For the Assessment of Safety Analysis and Design Software and Firmware
at Defense Nuclear Facilities

Topical Area:	**Objective:**
4.6 Software Quality Assurance	SQA activities are evaluated for applicability to the analysis and design software, defined to the appropriate level of rigor, and implemented.
Criteria	**Comments/Notes/ Results**
1. SQA activities and software practices for requirements management, software design, software configuration management, procurement controls, V&V (including reviews and testing), and documentation have been evaluated and established at the appropriate level for proper applicability to the analysis and design software under assessment.	
2. SQA activities have been effectively implemented.	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software Quality Assurance

Approach:

Determine if an appropriate SQA plan exists, either as a standalone document or embedded in another document, as well as related procedures, QA assessment reports, test reports, problem reports, corrective actions, supplier control, and training. Determine the effectiveness of the SQA program by reviewing the SQA plan. The assessment may also include interviewing managers, engineers, and software users. The SQA plan should identify:

- The software products to which it applies,
- The organizations responsible for maintaining software quality, along with their tasks and responsibilities,
- Required documentation: SRD, SDD, software user documentation, SCM plan, and software V&V plans and results,
- Standards, conventions, techniques, or methodologies that guide software development, as well as methods to ensure compliance to the same,
- Methods for error reporting and developing corrective actions, and
- Provisions for controlling software supplier activities for meeting established requirements.

Topical Area:	**Objective:**
4.7 Software Procurement	Vendor-supplied software, either COTS software, custom-developed or modified, requires the appropriate levels of QA commensurate with the level of risk introduced by their use.
Criteria	**Comments/Notes/ Results**
1. Procurement documents for acquisition of software programs identify the *functional, operational and* quality requirements appropriate for the level of risk introduced by their use.	
2. Acquired software is verified to meet the identified quality requirements.	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software Procurement

Approach:

Vendors that supply COTS and other software are evaluated to ensure that they develop software under an appropriate QA program and are capable of providing software that satisfies the specific requirements. The volume of commercial use for vendor software, especially with COTS software, should be considered in determining the adequacy of the vendor's QA program. The assessment of software procurements shall include the following:

- Determine the existence of acquired software QA requirements. These requirements may be embedded in the DOE contractor's or subcontractor's procurement requirements, SRD, SDD, or an SQA plan.
- Review the methods the site uses to verify that vender software meets the specified QA requirements, and determine if these methods accomplish those requirements. These methods may be included in an SQA plan or software test plan.
- Review evidence that the vendor software was evaluated for the appropriate level of quality. This evidence may be included in test results, a test summary, vendor site visit reports, or vendor QA program assessment reports.

Topical Area:	**Objective:**
4.8 Software Problem Reporting and Corrective Action	Formal procedures for software problem reporting and corrective action for software errors and failures are established, maintained, and controlled.
Criteria	**Comments/Notes/ Results**
1. Practices and procedures for reporting, tracking, and resolving problems or issues identified in both software items and software development and maintenance processes are documented and implemented. 2. Organizational responsibilities for reporting issues, approving changes, and performing corrective actions are identified and effective.	

Deleted: 16

Inserted: 16

Deleted: 16

Deleted: 16

Inserted: 16

Deleted: 16

Software Problem Reporting and Corrective Action

Approach:

Review documents and interview facility staff responsible for problem reporting and notification to determine if:

- A formal procedure exists for software problem reporting and corrective action development that addresses software errors, failures, and resolutions
- Corrections and changes are executed according to established change control procedures
- The problems that impact the software’s operation are promptly reported to affected organizations
- Corrections and changes are evaluated for impact and approved before being implemented
- Corrections and changes are verified for correct operation and to ensure that no side effects were introduced before being implemented
- Preventive measures and corrective actions are provided to affected organizations in a timely manner commensurate with the impact of the original defect
- The organizations responsible for problem reporting and resolution are defined